SHORT FORM SSAA

Instructions:

This Short Form (SF) System Security Authorization Agreement (SSAA) template is to be used for all DoDIIS systems designated as Director of Central Intelligence Directive (DCID) 6/3. The purpose of the SF SSAA is to describe security-relevant features of the system in support of security certification and accreditation within the DoDIIS Enterprise. The SF SSAA is normally added to a Site SSAA, which provides details surrounding the secure operation of the Site as a whole. The SF SSAA must be updated throughout a system's life cycle when significant, security-relevant changes take place.

For DoDIIS Enterprise systems, one overarching SF SSAA should be completed by the Program Management Office. If differences are identified at individual installation locations, these differences should be documented in an annex to the System SF SSAA. In addition, it is recommended that the SF SSAA be posted on Intelink, along with other Program Management Office information, for accessibility by the entire DoDIIS community.

Send all certification requests to the Independent Test Authority (ITA) to enter the DoDIIS certification process.

The SF SSAA may be classified due to overall content.

1. System Identification.

Information System Name	
Information System Number (if applicable)	
Date of SF SSAA	
Revision/Version	
Web Location for system documentation	
Security Test & Evaluation Date	

2. Primary System Points of Contact.

Function	Organizational POC	EMAIL Address	Contact Phone
Program Manager			
Designated Approval Authority			
Information Assurance Manager			
Information Assurance Officer			
System Administrator			

3. Data Processed. Identify the data to be processed, including classification levels and any relevant compartments and special handling restrictions. Check all boxes that apply to the classification or handling caveats of data processed on the information system.

Classification and Compartments:			
	UNCLASSIFIED		SI
	CONFIDENTIAL		TK
	SECRET		G
	TOP SECRET		OTHER
Dissemination Controls:			
	FOR OFFICIAL USE ONLY		ORCON
	REL TO:		HCS
	NOFORN		OTHER

4. **Protection Level and Level of Concerns.** Select the security protection level and the level of concern for Integrity and Availability (see DCID 6/3 Chapters 4, 5, and 6).

Confidentiality:					
	High				
Integrity					
	High		Medium		Low
Availability					
	High		Medium		Low

5. System Configuration.

a. System Description. Provide an executive summary/short description of the primary mission of the system.

b. Connectivity/Communications Links.

Direct Network Connections		
Check all boxes that apply to electronic connections with other systems		
	This system does not connect with any other system.	
	This system connects with another network or system(s) (list below).	
Provide the system name(s), classification/compartment level(s), and accreditor		
System Name	**Classification/Compartments**	**Accreditor**

c. Data Flow. Attach a diagram showing the logical connectivity and data flows for this system.

d. User Access Control. If Passwords are used to control access, complete the blocks below, checking all that apply. Otherwise, describe how user access control is provided.

	All users have their own unique userid and unique password
	Some users share a userid and password (explain below)
	Some users share a password (explain below)
	Privileged users with remote access to the information system use strong authentication
	All privileged users have their own unique userid and unique password
	Some privileged users share a userid and password (explain below)
	Some privileged users share a password (explain below)
	Users can change their passwords but are not forced to change their passwords on any timely basis, i.e., passwords are changed whenever the user feels it necessary
	Users are forced to change their passwords every (check all below that apply)
	30 Days 90 Days 180 Days Annual Never After Initial Login Other:
	Passwords are generated by the user
	Passwords generated by the user are validated through the use of automated tools
	Users are required to use strong passwords generated by the system
	Passwords are generated by an automated tool
	Passwords are provided by an access control manager
	If a user enters the wrong userid or password, a time-out of minutes is enforced
	If a user enters the wrong userid or password, the maximum number of attempts is
	If the maximum number of failed attempts is reached the user:
	If the maximum number of failed attempts is reached, the user may continue indefinitely
	Other (specify):
	If a user's account is locked out due to excessive invalid logon attempts, who is authorized to reinstate the account?
	Sys Admin IAM Privileged User Account Owner Any User
	System automatically reinstates the account after a specified time period

e. System Audits. Complete the blocks below.

Check the boxes corresponding to the information provided for the audited events					
	Userid		Type of event or action		Success/failure of event
	Time		Terminal or W/S ID		System location of event
	Date		Resources		Entity that initiated event
	Other:		Remote Access		Entity that completed evt

EVENT DESCRIPTION	**Do You Audit**	
	SUCCESS	**FAILURE**
Login’s		
Logoff’s		
Printing		
Copying of data to removable media		
Use of privileged user or root privileges		
Reading a file or directory		
Creation of a directory, file, or data element		
Deletion of a directory, file, or data element		
Attempts to change data		
Security relevant directories, objects, and incidents		
System console activities		
Information downgrades and overrides		
Change of user’s formal access permissions		
Attempted access to objects or data whole labels are inconsistent with user privileges		
Changes to security labels		
		YES/NO
Does the system have the capability to shut down in case of audit system failure?		
Does the system notify the ISSO of suspicious events?		
Does the system take the least disruptive action to terminate a suspicious event?		
How long is the audit log maintained on-line?		
How is the audit log maintained off-line?		

f. Remote Diagnostics/Remote Maintenance. Identify any requirement to perform remote diagnostics or remote maintenance of the system, and how this will be done in accordance with DCID 6/3 requirements.

g. Remote Access. Describe any user remote access envisioned for this system.

h. Software. Specify the operating system, system applications software and any special add-on security packages used, and describe the functions of each.

Software Name	Manufacturer	Vers/Rel	Purpose of Software	Server/Workstation Name where Software will be Installed

i. Hardware. Specify the following.

System Component Name	Manufacturer	Model Number	Nomenclature	QTY	Owned or Leased	Fixed or Removable Hard Drive

j. Ports and Services/Mobile Code Information. Provide the specified information required by the system. Agent/Mobile Code technology includes JAVA, Active X. etc.

Server Name	Port #/Services Required	Agent/Mobile Code Technology	Software component name using the port/service
Justification:			
Justification:			
Justification:			

k. General Information. Yes or no. If the answer is yes, please provide an explanation.

	YES/NO
Will the system store the data it acquires or processes?	
Does the system require a controlled interface (e.g., firewall)?	
Is the system web based?	
Is the system server to client?	
Is the system server to server? (no user interface)	
Does the system require SSL and has SSL been enabled on the system?	
Does this system require PKI and has PKI been enabled on the system?	
Explanation:	

6. Other Factors. Identify any peculiarities of the facility or IS which affects or may affect certification. Include any information which has a bearing on risk assessment. State any relevant physical, personnel, communications, or administrative security factors not provided in other sections of this submission.

7. Test and Evaluation Reports. Provide as an appendix to this SSAA Short Form.

8. System Security Certification. The Program Manager certifies:

"I certify that this IS conforms to the requirements specified in DCID 6/3 and the Joint DoDIIS Cryptologic SCI Information Systems Security Standards."

PM Signature